Consolidated Technology Services • WA

Incident Management/Notification Changes

	Current	Issues	Proposed Changes
Input	The CTS Service Desk receives a phone call or email from the customer. The Service Desk follows the procedure for support, creates a ticket, and performs associated support tier 1 support. When there is an unresolved incident the service desk notifies the appropriate CTS Service Back Office (technical support group).	While the Service Back Office is investigating the problem, the Service Desk may be receiving additional calls on the same problem. Until CTS begins issuing Incident Notifications, customers do not know if CTS is aware of the issue.	The CTS Service Desk uses the Automated Call Distribution (ACD) system to support the Service Desk function. The proposed change is to have the ACD message updated to inform subsequent callers with a message that CTS is aware of a current situation (e.g.: "We are currently receiving a high volume of calls reporting an issue with _____ ".) The message can optionally request special action by the customer, based upon circumstances (e.g.: provide specific needed information, take mitigating action, etc.). (Also, see #2 below)
Process	The CTS Service Back Office makes the determination if the event qualifies as a Major Incident (Severity 2).	There can be delays in implementing the escalated notification that major incidents (Severity 2) require. There can be a lack of consistency in timing and message content.	CTS is implementing a standardized, more rigorous Incident Response process modeled upon COOP and the Security Operations Center (SOC). The expected result is quicker escalation and more consistent messaging (through 'kiting' of message templates, and 'successive check' by Incident Commander).
Output	The Service Desk uses email to communicate Major Incidents. For incidents that involve email outage, they also contact agency help desks by phone. An out-of-band solution is in place for notifying CIOs during disaster (Severity 1) situations.	Email is not always available during an incident. Out-of-band messaging needs more granularity.	1) A more robust out-of-band solution is being investigated for use in Severity 1 and 2 incidents. It can send email and/or text messages to different distributions, based upon incident severity. 2) A web-based location (portal) is being configured to allow customers to check current status on any suspected or confirmed Severity 1 or 2 incident .